AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

starvoyager1108@gmail.com (TARGET ACCOUNT #1)
and teegeajw@gmail.com (TARGET ACCOUNT #2)

Case No. MJ18-407

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Target Accounts as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 2252(a)(1)	Transportation of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of child pornography

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SPECIAL AGENT INGRID ARBUTHNOT-STOHL, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 09/04/18

Judge's signature

City and state: SEATTLE, WASHINGTON

JOHN L. WEINBERG, U.S. MAGISTRATE JUDGE
Printed name and title

2018R00343

ATTACHMENT A

Place to be Searched

This warrant applies to information associated with the Google accounts starvoyager1108@gmail.com (TARGET ACCOUNT #1) and teegeajw@gmail.com (TARGET ACCOUNT #2), as well as all other subscriber and log records associated with the TARGET ACCOUNTS, and any preserved data, which is stored at premises owned, maintained, controlled, or operated by Google Inc., an electronic communications services and remote computing services provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

ATTACHMENT B

I. Section I - Information to be disclosed by Google for search:

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any emails, records, files, logs, or information that has been deleted but is still available to Google. Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. Google Chrome Browser history including but not limited to all search engine searches, as well as all URLs accessed (whether direct typed or linked from a search engine or other referring page). This information should include search suggestions and any searches that were typed by the user but that did not render results. This history should include date and time stamps associated with this activity.

b. List of devices that have accessed this user's Google account including any and all identifiers of the device such as Universal Unique Identifier (UUID), IMEI, operating system, etc.

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email, and any attachments to such emails;

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. The types of service utilized;

f. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, instant messages, and instant messenger contact information, calendar data, pictures, and files.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

II. Section II - Information to be seized by the government

All information described above in Section I that constitutes contraband, evidence, fruits, or instrumentalities of the following crimes committed on or after January 1, 2016: 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography)and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography):

h. All Google Chrome Browser history related to depictions of minors engaged in sexually explicit conduct (whether direct typed or linked);

a. List of devices that have accessed this user's Google account including any and all identifiers of the device such as UUID, IMEI, operating system, MAC address,

b. All email or other communications related to visual depictions of minors engaged in sexually explicit conduct or the sexual exploitation/abuse of minors;

c. All visual depictions of minors engaged in sexually explicit conduct;

d. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

e. Any address lists or buddy/contact lists associated with the specified account;

f. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

g. Any and all other log records, including IP address captures, associated with the specified account; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

h. Any records of communications between Google and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

Notwithstanding the criminal offenses defined under 18 U.S.C. § 2252 and 2252A or any similar criminal offense, Google shall disclose information responsive to this warrant by mailing it to Federal Bureau of Investigation, Attn: Special Agent Ingrid Arbuthnot-Stohl at 1110 Third Avenue, Seattle, WA 98101, or via email to iarbuthnot-stohl.fbi.gov.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

AFFIDAVIT

STATE OF WASHINGTON) ss
COUNTY OF KING)

I, Ingrid Arbuthnot-Stohl, being duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the Special Agent in Charge in Seattle, Washington. I have been an Agent with the FBI since December 2010. As part of my daily duties as an FBI agent, I investigate criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code §§ 2251(a), 2252A, 2422, and 2423. I have received training in the area of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography in numerous forms of media, including media stored on digital media storage devices such as computers, iPhones, etc. I have also participated in the execution of numerous search warrants involving investigations of child exploitation and/or child pornography offenses. I am a member of the Seattle Internet Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

2. I make this affidavit in support of an application for a search warrant for information associated with certain accounts starvoyager1108@gmail.com (TARGET ACCOUNT #1) and teegeajw@gmail.com (TARGET ACCOUNT #2) that is stored at premises controlled by Google, an e-mail provider headquartered at 1600 Amphitheatre Parkway Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. The facts set forth in this Affidavit are based on the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation. I have set forth only the facts I believe are relevant to the determination of probable cause to believe evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) will be found in the TARGET ACCOUNTS.

BACKGROUND

5. In March 2001, Anthony J. Weir pleaded guilty to several criminal charges involving the sexual exploitation of three minors and the possession of child pornography: Count 1 and 2 in the Western District of Washington of sexual exploitation of a minor, Jane Doe 1 and 2, in violation of Title 18, United States Code, Section 2251(a) and (d); Count 3 in the Southern District of Ohio to transfer in interstate commerce of obscene matter to a minor, Jane Doe 3, in violation of Title 18, United States Code, Section 1470; Count 4 in the Southern District of Ohio of use of a facility of means of interstate commerce to attempt to persuade, induce, entice and coerce a minor, Jane Doe 3, to engage in sexual activity for which any person can be charged with

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

a criminal offense, in violation of Title 18, United States Code, Section 2422(b); Count 5 in the Western District of Washington of possession of child pornography in violation of Title 18, United States Code, Section 2252A(a)(5)(B) and (b)(2). Weir entered into a plea agreement with the United States as part of these guilty pleas and agreed to a lengthy factual statement, which I summarize below:

Jane Doe 1 (10 years old): Sometime in May 2000, Jane Doe 1's aunt, who was dating Weir, brought her to Weir's home. Weir said Jane Doe 1 was "cute" and wanted to photograph her for his "toy web-site." Weir took Jane Doe 1 into his bedroom and proceeded to take photos of Jane Doe 1 in which her genitalia were exposed to the camera. Once he was finished, Weir gave Jane Doe 1's aunt a sum of money, purportedly for Jane Doe 1.

Jane Doe 2 (12 years old): In June 2000, Weir took nude photographs of Jane Doe 2 in the bedroom of his home while Jane Doe 2's mother was in the other room. Weir had met Jane Doe 2's parents at a tavern on an earlier date and told them that he wanted to feature Jane Doe 2 on a website for selling children's toys he was building.

Jane Doe 3 (13 years old): Weir and Jane Doe 3 began an online relationship in the fall of 1998 when Jane Doe 3 was approximately 13. From that time until March 2000, Weir and Jane Doe 3 communicated by phone and internet messaging and exchanged sexually explicit messages and engaged in telephone sex. On at least one occasion, Weir sent Jane Doe 3 a picture of himself in which he was wearing a cowboy hat and nothing else. In the picture, his penis was partially erect. Weir also encouraged Jane Doe 3 to engage in sexual activity with her younger half-brother.

July 2000: Following the execution of a search warrant at his home, police found that Weir had roughly 200 floppy disks containing visual depictions of minors engaged in sexually explicit conduct.

6. Following entry of his guilty pleas in the United States District Court for the Western District of Washington, Weir was sentenced to 210 months' imprisonment and 5 years of supervised release.

III. SUMMARY OF INVESTIGATION

7. This investigation originated with the United States Probation Office (USPO) in Seattle, Washington. I reviewed reports and other information provided by

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

USPO, and the following is a summary of information and a chronology of events gleaned from those reports/information.

- Weir began supervision in the Western District of Washington in October 2015. Officer Erin O'Donnell started supervising Weir in October 2017. Among his conditions of supervision, Weir 1) was required to submit his person, property, and residence to search by U.S. Probation; 2) submit to polygraph examinations; and abide by lifestyle restrictions proscribed as part of his sexual deviancy treatment. In addition, Weir was prohibited from having internet access and not permitted to have pornographic material.

- November 8, 2017: Officer O'Donnell conducted a routine home inspection, during which she noted Weir had senior portraits of a blonde female, and a locked safe. Both of the objects were positioned so they could not be seen from the doorway. Officer O'Donnell took note of this because the officer who supervised Weir previously usually conducted routine inspections standing in the doorway.

- November 9, 2017: Officer O'Donnell discussed this issue with Weir's treatment provider, Dan Knoepfler, and Senior United States Probation Officer Sarah Cavendish, a sex offender specialist. It was determined to address the issues of the photographs and the safe via polygraph.

- December 7, 2017, and January 15, 2018: Officer O'Donnell conducted routine home inspections, during which she inquired about the contents of the safe, and if the contents would place Weir in violation. Weir claimed it contained legal documents he did not want jeopardized and denied violation behavior.

- January 31, 2018: Weir was found deceptive on a polygraph question related to his honesty about the contents of the safe. Deception on this question made the results of the second question, related to the senior portraits, invalid.

- February 1, 2018: The case was staffed with Supervising United States Probation Officer Jerrod Akins, Search Team Coordinator. Reasonable suspicion to conduct the search was based on Weir's criminal history, concealment of unknown content, the circumstances surrounding the senior portraits, and the deceptive results of the polygraph. A request to conduct a search of Weir's residence was submitted to and approved by Chief United States Probation Officer Connie Smith.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

- February 7, 2018: An approved search was conducted by USPO with the assistance of Seattle Police Officer Ian Polhemus and K9 Bear. USPO confiscated several digital devices, an LG smartphone.

- February 7, 2018: Officer O'Donnell submitted a follow up search request to Chief United States Probation Officer Connie Smith to search the contents of the Black LG G6 phone, serial #355468-08-036997-8 (an internet-capable smartphone), which was approved. Further reasonable suspicion was developed due to Weir's failure to disclose the phone, the location of the phone, his attempts to prevent probation from accessing it, and the varying reasons he provided for why he could or would not provide the passwords to it. The follow-up search was focused on this phone due to its location under Weir's pillow, with charging cords nearby.

- March 13, 2018: Senior United States Probation Officer Matthew McDaniel was able to access some of the files on an SD card in the Black LG G6 phone, serial #355468-08-036997-8, and determined from his experience the files contained images of child pornography. USPO then sought and obtained a warrant for Weir's arrest based on alleged violations of his conditions of supervision.

- March 20, 2018: United States Deputy Marshal John Westland took Weir into custody on the warrant. On Weir's person, Deputy Westland located a blue flip phone and a second LG smartphone.

8. U.S. Probation conducted a preliminary forensic examination of the LG smartphone seized from Weir's residence on February 7, 2018. I summarize his report of that examination below:

- Officer McDaniel has been employed with United States Probation since 1999, and in his current capacity serves as a Senior United States Probation Officer, Sex Offender Specialist. Officer McDaniel supervises a caseload of high-risk sex offenders and is responsible for conducting forensic examinations on all digital media and devices within the Western District of Washington. Officer McDaniel has served as the District's only forensic examiner since 2000. He has completed over 700 hours of formal computer forensic training, has held forensic examiner certifications, and has been accepted as an expert witness on this topic in United States District Court. Officer McDaniel has been involved in the supervision of many child pornography offenders throughout his career, and has conducted dozens of forensic examinations on devices used by child pornography offenders.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

- Following a search of Anthony Weir's residence by United States Probation, Officer McDaniel received a number of cell phones, along with other items of potential evidentiary value. Based upon a request from the supervision officer, Erin O'Donnell, Officer McDaniel began to review these devices for potential forensic examination. One phone, an LG G6 smartphone, was considered the primary investigative target by Officer O'Donnell. Officer McDaniel attempted on two occasions to complete a forensic examination of this device using Cellebrite hardware but was unsuccessful due to the device's user-enabled encryption. USPO attempted to obtain the passcodes for the device from Weir, who refused to provide them.

- On March 13, 2018, Officer McDaniel conducted a second visual examination of Weir's LG G6 smartphone. Officer McDaniel had visually examined the phone on a prior occasion in order to attempt to conduct a forensic examination of the phone itself. However, based upon the encryption configured by the owner (LG's secure boot was enabled), Officer McDaniel was unable to complete the exam which was focused on the phone's internal storage. At that time, Officer McDaniel did not see any removable SD card slots or a removable back panel where a micro SD card is typically stored. During his subsequent examination of the phone, Officer McDaniel used a small pin to remove the cover for the SIM card as he noticed that the sim card cover was a bit larger than usual. Upon doing so, he found a 64GB micro SD storage card within the phone. No serial number was present on the micro SD card, but the card was located in a slot next to a T-Mobile SIM card with ID#: 8901260873756510000.

- Officer McDaniel conducted an initial inspection of the SD card using a write-protected hardware device to determine whether any data was present, and if so, whether an in-depth forensic examination was warranted. Officer McDaniel viewed the folder structure and identified dozens of folders on the root of the SD card, many of which were labeled with female names. USPO McDaniel opened a few random folders and worked his way down the folder structure. The first few folders contained screenshots of what appeared to be a paystub from a temporary employment service addressed to "Anthony Weir". Another folder, named "Gallery" contained a series of sub-folders, one of which was named "Screenshots"

- Within the "Screenshots" folder, Officer McDaniel observed approximately two dozen images of pre-pubescent female children who appeared to be standing and/or lying on a bed. USPO McDaniel's basis for categorizing these images as "pre-pubescent" is the lack of visible breast development, the stature/physical size

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

of the individuals, and facial features. The females were partially clothed (in underwear or a t-shirt) in several of the photos, and some of these photos were taken in a manner to focus upon the pubic area. One image depicted what is believed, based upon Officer McDaniel's experience, to be a minor-aged female lying on a bed with her feet facing the camera. She is lying on her back in a t-shirt and underwear, her knees are bent and her legs are spread to display her pubic area. The image is clearly centered upon the pubic area of this individual.

- Another image was of a slightly dark-skinned, dark-haired female, clearly pre-pubescent (based upon lack of visible breast development and small stature), who is facing the camera. The background of the shot depicts a white/off-white wall which could be a shower stall or bathroom wall. The individual is portrayed from the waist up, and is nude. The breasts and face of this individual are clearly visible.

- Based upon Officer McDaniel's experience as a forensic examiner and a supervision officer assigned to sex offenders, he has seen a number of images that are known to be "child pornography". Many child pornography images are usually taken in a photo series, with the victims displayed in various states of undress and in various poses/activities. The images Officer McDaniel viewed on Weir's SD card are consistent with these types of images, and once he observed the image depicting the topless pre-pubescent female, he immediately discontinued the search and referred the matter back to Officer O'Donnell for referral to law enforcement.

9. On March 28, 2018, I appeared before the Honorable Paula L. McCandlis and obtained a warrant to search and forensically examine digital devices seized from WEIR during the USPO search and on the day of his arrest. Among the devices whose contents I have reviewed is a SanDisk SD card removed from WEIR's LG G6 smartphone. On the back of the SD card is stamped "Made in Taiwan."

10. Located on this device are approximately 23 images of prepubescent females engaged in sexually explicit conduct. More specifically, these images depict prepubescent females in various stages of undress and involve the lascivious exhibition of the genitals or pubic area those females. I describe two such images below:[1]

[1] On April 20, 2018, I appeared before Magistrate Judge Mary Alice Theiler and applied for an arrest warrant for Anthony J. WEIR. In support of that request, I submitted a criminal complaint and provided copies of the two

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

screenshot_2018-02-03-22-59-42.png: This is an image of a prepubescent female approximately 8 years old based upon overall body structure/size, lack of hip/breast development, lack of pubic hair, and facial features. She is standing in a bathroom, and the picture is a voyeur type of shot that is taken from the hallway. The minor is wearing pajamas with the top pulled up and the bottoms pulled to fully expose her vaginal area to the camera. She appears to be trying to sit down on the toilet. The minor appears to be surprised, and her expression suggests she was not aware she would be photographed.

screenshot_2017-10-31-11-21-47.png: This is an image of a prepubescent female approximately 11 years old based upon overall body structure/size, facial features, and lack of hip/breast development. The minor is facing the camera, and the shot appears to be a webcam capture. She is standing on one leg with the other leg straight up in the air. She is wearing short shorts that just barely cover her genitals. However, the focus of the picture is her groin.

11. Following his arrest in April 2018, a Grand Jury sitting in the Western District of Washington has indicted WEIR on a single count of possession of child pornography in Cause No. CR18-108RSL.

12. I reviewed a Silver LG G6 cell phone, IMEI: 355468-08-036997-8 that contained the SD card referenced above with the 23 images of child pornography that was seized by US Probation and for which I obtained a search warrant. The device data showed it was used to access the email account teegeajw@gmail.com (TARGET ACCOUNT 2). In addition, I reviewed a red and black Android cell phone, also seized by US Probation and included in the previously referenced search warrant. The device data showed it was used to access the email account starvoyager1108@gmail.com (TARGET ACCOUNT 1). TARGET ACCOUNT 1 is associated with other Google services like Google+, Google Drive, Google Chrome, and Hangouts. WEIR is the only known user of these two devices.

---

images described in this paragraph to the magistrate judge as exhibits. Those exhibits were filed under seal in Case No. MJ18-182 and are in the custody of the United States Attorney's Office for the Western District of Washington. If requested, I will arrange to make these exhibits available to the reviewing magistrate judge as part of this search warrant application.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

13. I served Google with administrative subpoenas seeking subscriber information and IP connection logs for TARGET ACCOUNTS 1 and 2. The information provided by Google included the following:

TARGET ACCOUNT 1 (starvoyager1108@gmail.com)
Name: Antonio J
Created on: 2016/08/13-04:21:30-UTC

TARGET ACCOUNT 2 (teegeajw@gmail.com)
Name: Anthony W.
Created on: 2015/09/02-20:51:56-UTC

SUBJECT'S USE OF ELECTRONIC COMMUNICATION SERVICES

14. In my training and experience, I have learned that Google is a technology company that offers a variety of Internet-related services and products. Google is most commonly known as a search engine, however, Google also offers cloud storage (Google Drive), email (Gmail), social networking (Google+), and photo organizing (Google Photos). Google is also responsible for the development of the Google Chrome web browser.

15. Google's Chrome web browser is an application that allows a user to access the Internet. Just as with any other browser, Google Chrome allows the user to type a URL directly to access a website or use a search engine to locate a desired website. Relevant here are the Google and Bing search engines. Both of these search engines allow the user to narrow the scope of a search to a particular type of material such as maps, images, etc.

16. Results from Google Search are populated by data from the Internet that have been indexed. Google and has automated programs called "bots" or "crawlers" that locate web URLs and index the information for retrieval by users of the search engine. Any user with Internet access can use a web browser and search engine to locate indexed web pages. The method of crawling and indexing is complicated and based on proprietary coding. Search results are largely based on metadata or tags associated with

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

the image, such as the image's title. For example, a Bing Images search for "sunset" will typically render pictures of a sunset but may also render images of a t-shirt showing a sunset that is titled, "sunset t-shirt.jpg"

17. When a user logs into his/her Google account (such as Gmail) via Google Chrome and then accesses the web, his/her personal browsing data are saved on Google's servers and synced with that account. This saved information includes browsing history, bookmarks, tabs, and browser settings. The Google Chrome browser is defaulted to automatically sync the browsing history, bookmarks, tabs, and browser settings to each device when a user logs in. If set to the default, these settings are therefore automatically loaded anytime the user signs into Google on other computers and devices. The user can customize what information is synchronized, however, the default method is to store all information as listed above.

18. Users often stay logged into their Google account even after the browser is closed and then re-launched. Logging out of Google takes an affirmative action to click on an icon and select "log out." For this reason, many users stay logged into their Google account constantly. If a user is logged into Google and accesses a webpage, Google stores this information as associated with the account. If a user accesses B Google search engines, Google stores this information associated with their account.

19. Google subscribers obtain an account by registering with Google. When doing so, e-mail/online services providers like Google ask the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users, and to help establish who has dominion and control over the account.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

20. E-mail/online services providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account, which can help establish the individual or individuals who had dominion and control over the account

21. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google's servers for a certain period of time.

22. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often maintains a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google server, the e-mail can remain on the system indefinitely. Even if the sender deletes the e-mail, it may continue to be available on Google's servers for a certain period of time.

23. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

it, that message may also be saved by Google but may not include all of these categories of data.

24. A Google subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, photographs, and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, attachments to e-mails, including photographs and files, and photographs and files stored in relation to the account.

25. A subscriber to a Google Gmail account can also store files, including address books, contact lists, calendar data, photographs and other files, on servers maintained and/or owned by Google. For example, Google offers users a calendar service that users may utilize to organize their schedule and share events with others. Google also offers users' a service called Google Drive that may be used to store data and documents. The Google Drive service may be used to store documents including spreadsheets, written documents (such as Word or Word Perfect) and other documents that could be used to manage a website. Google Drive allows users to share their documents with others or the public depending on the settings selected by the account holder. Google also provides its users with access to the photo storage service "Google + Photos," formerly known as Picasa. Google + Photos can be used to create photo albums, store photographs, and share photographs with others. Another Google service called "You Tube" allows users to view, store and share videos. Google also provides a service called "Google Analytics. Google Analytics is a Google service that monitors website traffic and provides subscribers with data relating to how much traffic is visiting the subscriber's website, which sections of the subscriber's website users are visiting, how long users are staying on particular sections of the site, and the geographical source of users visiting the website, among other things. Another Google service called "Google Hangouts" is a communication platform which includes instant messaging, video chat, short message service (SMS) and voice over internet protocols (VOIP) features.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

26. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

27. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly. They also may opt to store the contraband in cloud accounts. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage can span multiple servers, and often locations, and the physical environment is typically owned and managed by a hosting company. Cloud storage allows the offender ready access to the material from any device that has an Internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender's device.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. E-mail itself provides a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

stored on email "cloud" servers, which allow users to store a large amount of material at no cost, without leaving any physical evidence on the users' computer(s).

28. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

29. Given the above-stated facts, including WEIR's criminal history and his conduct while on federal supervision, and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that WEIR is a user or owner of the TARGET ACCOUNTS and likely has a sexualized interest in children and depictions of children. I therefore believe that evidence of child pornography is likely to be found on the TARGET ACCOUNTS.

PAST EFFORTS TO OBTAIN EVIDENCE FROM THE SUBJECT ACCOUNTS

30. I understand the contents of the TARGET ACCOUNTS can only be obtained, in the Ninth Circuit, by means of a search warrant issued under authority of 18 U.S.C. § 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and Federal Rule of Criminal Procedure

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

41(e)(2)(b). On or about October 19, 2017, I sent a preservation letter to Google, requesting they preserve the contents related to TARGET ACCOUNTS.

GENUINE RISKS OF DESTRUCTION OF EVIDENCE

31. Based upon my experience and training, it is not uncommon for technically sophisticated criminals to use encryption or programs to destroy data which can be triggered remotely or by a pre-programed event or keystroke, or other sophisticated techniques to hide data. In this case the data sought is stored on a server belonging to Google. If data is accessed and deleted by the user, by either deleting the emails or any associated contact lists, the content would not be retrievable. Unlike traditional computer forensics where a hard drive can be searched and deleted documents recovered, information stored in an enterprise storage system is irretrievable once it has been deleted. Further, since this information is accessible from anywhere the suspect can obtain an Internet connection to log on to his account, he can delete this information in a matter of minutes. Moreover, if agents ask the owner of the TARGET ACCOUNTS for consent to search it, he may refuse to consent to such a search and then destroy evidence in the TARGET ACCOUNTS before agents are able to obtain a search warrant.

PROTOCOL FOR SORTING SEIZABLE ELECTRONICALLY STORED INFORMATION

32. In order to insure agents are limited in their search only to the contents of the TARGET ACCOUNTS and any attachments, stored instant messages, stored voice messages, documents, and photographs associated therewith; in order to protect the privacy interests of other third parties who have accounts at Google; and in order to minimize disruptions to normal business operations of Google; this application seeks authorization to permit agents and employees of Google to assist in the execution of the warrant, pursuant to 18 U.S.C. § 2703(g), as follows:

a. The search warrant will be presented to Google, with direction that it identify and isolate the TARGET ACCOUNTS and associated records described in Section I of Attachment B.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

b. Google will also be directed to create an exact duplicate in electronic form of the TARGET ACCOUNTS and associated records specified in Section I of Attachment B, including an exact duplicate of the content of all email messages stored in the TARGET ACCOUNTS.

c. Google shall then provide an exact digital copy of the contents of the TARGET ACCOUNTS, as well as all other records associated with the account, to me, or to any other agent of FBI. Once the digital copy has been received from Google, that copy will, in turn, be forensically imaged and only that image will be reviewed and analyzed to identify communications and other data subject to seizure pursuant to Section II of Attachment B. The original digital copy will be sealed and maintained to establish authenticity, if necessary.

d. I, and/or other agents of FBI will thereafter review the forensic image, and identify from among the content those items which come within the items identified in Section II to Attachment B, for seizure. I, and/or other agents of FBI will then copy those items identified for seizure to separate media for future use in investigation and prosecution.

e. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords search text, and many common electronic mail, database, and spreadsheet applications (which may be attached to email) do not store data as searchable text. The data is saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases as well. Consistent with the foregoing, searching the recovered data for the information subject to

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months.

f. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to seize all emails, chat logs and documents, which identify any users of the subject account and any emails sent or received in temporal proximity to incriminating emails which provide context to the incriminating communications.

g. All forensic analysis of the image data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

CONCLUSION

33. Based upon the evidence gathered in this investigation as set out above, including but not limited to my review of data and records, information received from other law enforcement agents, and my training and experience, there is probable cause to believe evidence, fruits and/or instrumentalities of the crimes of 18 U.S.C. § 2252(a)(1) (Transportation of Child Pornography) and 18 U.S.C. §§ 2252(a)(4)(B) (Possession of Child Pornography) exists and will be found in the electronically stored information or communications contained and associated with the TARGET ACCOUNTS and any attachments, stored instant messages, stored voice messages, documents, and photographs associated therewith, as well as in subscriber and log records associated with the account. Accordingly, by this Affidavit and warrant I seek authority for the government to search all of the items specified in Attachment A and Section I of Attachment B and specifically to seize all of the data, documents and records which are identified in Section II of Attachment B.

INGRID ARBUTHNOT-STOHL
Special Agent, FBI

Subscribed and sworn to before me this 4 day of ~~August,~~ September 2018.

JOHN L. WEINBERG
United States Magistrate Judge

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

ATTACHMENT A

Place to be Searched

This warrant applies to information associated with the Google accounts starvoyager1108@gmail.com (TARGET ACCOUNT #1) and teegeajw@gmail.com (TARGET ACCOUNT #2), as well as all other subscriber and log records associated with the TARGET ACCOUNTS, and any preserved data, which is stored at premises owned, maintained, controlled, or operated by Google Inc., an electronic communications services and remote computing services provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

ATTACHMENT B

I. Section I - Information to be disclosed by Google for search:

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any emails, records, files, logs, or information that has been deleted but is still available to Google. Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. Google Chrome Browser history including but not limited to all search engine searches, as well as all URLs accessed (whether direct typed or linked from a search engine or other referring page). This information should include search suggestions and any searches that were typed by the user but that did not render results. This history should include date and time stamps associated with this activity.

b. List of devices that have accessed this user's Google account including any and all identifiers of the device such as Universal Unique Identifier (UUID), IMEI, operating system, etc.

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email, and any attachments to such emails;

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. The types of service utilized;

f. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, instant messages, and instant messenger contact information, calendar data, pictures, and files.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

II. Section II - Information to be seized by the government

All information described above in Section I that constitutes contraband, evidence, fruits, or instrumentalities of the following crimes committed on or after January 1, 2016: 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography)and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography):

h. All Google Chrome Browser history related to depictions of minors engaged in sexually explicit conduct (whether direct typed or linked);

a. List of devices that have accessed this user's Google account including any and all identifiers of the device such as UUID, IMEI, operating system, MAC address,

b. All email or other communications related to visual depictions of minors engaged in sexually explicit conduct or the sexual exploitation/abuse of minors;

c. All visual depictions of minors engaged in sexually explicit conduct;

d. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

e. Any address lists or buddy/contact lists associated with the specified account;

f. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

g. Any and all other log records, including IP address captures, associated with the specified account; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

h. Any records of communications between Google and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

Notwithstanding the criminal offenses defined under 18 U.S.C. § 2252 and 2252A or any similar criminal offense, Google shall disclose information responsive to this warrant by mailing it to Federal Bureau of Investigation, Attn: Special Agent Ingrid Arbuthnot-Stohl at 1110 Third Avenue, Seattle, WA 98101, or via email to iarbuthnot-stohl.fbi.gov.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970